PCT/JP2004/007017

日本国特許庁

18.5.2004

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　８月１１日

出願番号
Application Number: 特願２００３－２９１７４１

[ST. 10/C]: [ＪＰ２００３－２９１７４１]

出願人
Applicant(s): ソニー株式会社

２００４年　６月１８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０５２６５３

【書類名】　特許願
【整理番号】　0390573403
【提出日】　平成15年 8月11日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　H04L 9/32
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　村瀬　泰弘
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　守谷　淳
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082762
　【弁理士】
　【氏名又は名称】　杉浦　正知
　【電話番号】　03-3980-0339
【選任した代理人】
　【識別番号】　100120640
　【弁理士】
　【氏名又は名称】　森　幸一
【手数料の表示】
　【予納台帳番号】　043812
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0201252

【書類名】特許請求の範囲
【請求項１】
利用者が操作する認証を受ける複数の認証端末と、共通の認証サーバと、複数のサービス提供事業者とがネットワークを介して接続されたシステムにおける認証方法であって、
認証端末からユーザー認証の要求を受けた認証サーバが上記認証端末を操作する利用者の認証を行い、認証結果として生成されたデータを上記認証端末へ返却する第１認証ステップと、
上記認証端末からの認証チケット要求のデータを受けた上記認証サーバが認証チケット発行のための認証を行い、認証結果として生成された認証チケットを含むデータを上記認証端末へ返却する第２認証ステップと、
上記認証端末からの上記認証チケットを含むサービス提供要求のデータを上記認証端末から受けたサービス提供事業者サーバが上記認証チケットが正当なものかを判断するために行う第３認証ステップとからなり、
上記第３認証ステップは、上記サービス提供事業者自身が正当である事を証明するためのデータを含んだ認証チケット認証要求を上記認証サーバへ送信する送信ステップと、上記認証サーバで実行された認証結果を受ける事で認証チケットが正当なものかの判断する判定ステップと、上記判定ステップで生成されたデータを上記認証端末へ返却するステップとからなる認証方法。
【請求項２】
請求項１において、
上記認証チケットは、上記認証端末に対してのみ発行される一意で且つユーザ認証情報を含まないものである認証方法。
【請求項３】
請求項１において、
上記認証チケットは、一度しか使用できないものである認証方法。
【請求項４】
請求項１において、
上記認証チケットは、上記第１認証ステップで生成されてから上記第３認証ステップで上記認証サーバが上記認証チケットの認証を実行するまでの時間に対して有効時間が設定され、上記有効時間を経過すると無効とされるものである認証方法。
【請求項５】
請求項１において、
上記認証サーバは、利用者の利用履歴情報から抽出された利用者の嗜好情報のデータベースをさらに有し、
サービス提供事業者が上記認証サーバに対して広告情報および広告要求を送信し、
上記認証サーバは、上記広告情報と上記嗜好情報とを比較し、比較の結果一致した利用者に対してのみ上記広告情報を送信する認証方法。
【請求項６】
請求項１において、
上記認証サーバは、利用者の利用履歴情報から抽出された利用者の嗜好情報のデータベースをさらに有し、
上記認証サーバは、上記第２ステップにおいて、上記認証チケットを発行するときに、上記認証チケットと共に上記データベース内の上記嗜好情報を上記認証端末へ返却し、
上記利用者が上記サービス提供事業者にアクセスするときに、上記嗜好情報を送信する認証方法。
【請求項７】
利用者が操作する認証を受ける複数の認証端末と、共通の認証サーバと、複数のサービス提供事業者とがネットワークを介して接続された認証システムにであって、
認証端末からユーザー認証の要求を受けた認証サーバが上記認証端末を操作する利用者の認証を行い、認証結果として生成されたデータを上記認証端末へ返却する第１認証手段

と、
上記認証端末からの認証チケット要求のデータを受けた上記認証サーバが認証チケット発行のための認証を行い、認証結果として生成された認証チケットを含むデータを上記認証端末へ返却する第２認証手段と、
上記認証端末からの上記認証チケットを含むサービス提供要求のデータを上記認証端末から受けたサービス提供事業者サーバが上記認証チケットが正当なものかを判断するために行う第３認証手段とからなり、
上記第３認証手段は、上記サービス提供事業者自身が正当である事を証明するためのデータを含んだ認証チケット認証要求を上記認証サーバへ送信する送信手段と、上記認証サーバで実行された認証結果を受ける事で認証チケットが正当なものかの判断する判定手段と、上記判定手段で生成されたデータを上記認証端末へ返却する手段とからなる認証システム。
【請求項８】
利用者が操作する認証を受ける複数の認証端末と、複数のサービス提供事業者とネットワークを介して接続され、上記認証端末および上記サーバ提供事業者に対して共通の認証サーバであって、
認証端末からユーザー認証の要求を受け、上記認証端末を操作する利用者の認証を行い、認証結果として生成されたデータを上記認証端末へ返却する第１認証手段と、
上記認証端末からの認証チケット要求のデータを受け、認証チケット発行のための認証を行い、認証結果として生成された認証チケットを含むデータを上記認証端末へ返却する第２認証手段と、
上記認証端末からの上記認証チケットを含むサービス提供要求のデータを上記認証端末から受けたサービス提供事業者サーバが上記認証チケットが正当なものかを判断するために行う第３認証手段とからなり、
上記第３認証手段は、上記サービス提供事業者自身が正当である事を証明するためのデータを含んだ認証チケット認証要求を上記サービス提供事業者から受ける受信手段と、上記認証チケットが正当なものか否かを判断する判定手段と、上記判定手段で生成されたデータを上記サービス提供事業者に送信する手段とからなり、
上記サービス提供事業者が上記判定手段で生成されたデータを上記認証端末へ返却する認証サーバ。
【請求項９】
請求項８において、
上記認証チケットは、上記認証端末に対してのみ発行される一意で且つユーザ認証情報を含まないものである認証サーバ。
【請求項１０】
請求項８において、
上記認証チケットは、一度しか使用できないものである認証サーバ。
【請求項１１】
請求項８において、
上記認証チケットは、上記第１認証手段で生成されてから上記第３認証手段で上記認証サーバが上記認証チケットの認証を実行するまでの時間に対して有効時間が設定され、上記有効時間を経過すると無効とされるものである認証サーバ。
【請求項１２】
請求項８において、
上記認証サーバは、利用者の利用履歴情報から抽出された利用者の嗜好情報のデータベースをさらに有し、
サービス提供事業者が上記認証サーバに対して広告情報および広告要求を送信し、
上記認証サーバは、上記広告情報と上記嗜好情報とを比較し、比較の結果一致した利用者に対してのみ上記広告情報を送信する認証サーバ。
【請求項１３】

請求項８において、
上記認証サーバは、利用者の利用履歴情報から抽出された利用者の嗜好情報のデータベースをさらに有し、
上記認証サーバは、上記第２認証手段において、上記認証チケットを発行するときに、上記認証チケットと共に上記データベース内の上記嗜好情報を上記認証端末へ返却し、
上記利用者が上記サービス提供事業者にアクセスするときに、上記嗜好情報を送信する認証サーバ。

【書類名】明細書
【発明の名称】認証方法、認証システムおよび認証サーバ
【技術分野】
【０００１】
この発明は、シングルサインオンの認証方法、認証システムおよび認証サーバに関する。
【背景技術】
【０００２】
従来、インターネット上のサービス提供事業者（WWWサーバ）が提供するサービスの利用者認証はサービス提供事業者毎に行われ、利用者がサービス提供事業者と直接契約を結び、それぞれのサービス提供事業者の認証を受ける必要があった。これにより、利用者はサービス提供事業者毎の認証情報を記憶・定期的に更新する必要があったため、利便性は必ずしも良いものではなかった。
【０００３】
そこで、利用者が１回のログインで複数のサービス提供事業者にアクセス可能なシングルサインオンという方式が考案された。シングルサインオン方法によって、ユーザが複数のＩＤや、パスワードを記憶したり、更新する必要がなくなり、ユーザの負担が軽減される。また、認証を共通とできることは、システム管理者あるいはアプリケーション開発者にとっても負担が軽減される。しかしながら、従来の方式ではシステム構築面，セキュリティ面で以下のいくつかの問題点があった。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
１．サービス提供事業者は、シングルサインオン認証機能提供事業者が採用しているディレクトリサービスや、ある定められたシングルサインオン認証処理手順等と同期する必要があり、そのためのシステム構築，運用が必要であり、その分のコストも必要であった。
【０００５】
２．サービス提供事業者が複数のネットワークサービス提供事業者と契約して、複数のネットワークサービス提供事業者の利用者へ向けてサービスの提供を行う場合は、それぞれのネットワークサービス提供事業者のシングルサインオン認証方式に沿ったシステム構築，運用が必要であった。
【０００６】
３．利用者が、利用者ＩＤ／パスワードによるシングルサインオン認証（ユーザー認証）後、ユーザー認証サーバから送信されてくる認証許可され利用者を一意に特定する情報（以下、セッションＩＤ）を、利用者が使用する端末内に保存しておかねばならなかったため、セッションＩＤが盗まれ、他の端末から不正使用された場合、サービス提供事業者は正当な利用者からのアクセスかどうかの判別ができなかった。
【０００７】
４．１つのセッションＩＤで全てのサービスを受ける事ができるため、セッションＩＤが盗まれた場合、別の端末から、不正な利用者が全てのサービス提供事業者へアクセス可能であった。
【０００８】
したがって，この発明の目的は、これらの問題点が解決された認証方法、認証システムおよび認証サーバを提供することにある。
【課題を解決するための手段】
【０００９】
上述した課題を解決するために、この発明は、利用者が操作する認証を受ける複数の認証端末と、共通の認証サーバと、複数のサービス提供事業者とがネットワークを介して接続されたシステムにおける認証方法であって、

認証端末からユーザー認証の要求を受けた認証サーバが認証端末を操作する利用者の認証を行い、認証結果として生成されたデータを認証端末へ返却する第１認証ステップと、
認証端末からの認証チケット要求のデータを受けた認証サーバが認証チケット発行のための認証を行い、認証結果として生成された認証チケットを含むデータを認証端末へ返却する第２認証ステップと、
認証端末からの認証チケットを含むサービス提供要求のデータを認証端末から受けたサービス提供事業者サーバが認証チケットが正当なものかを判断するために行う第３認証ステップとからなり、
第３認証ステップは、サービス提供事業者自身が正当である事を証明するためのデータを含んだ認証チケット認証要求を認証サーバへ送信する送信ステップと、認証サーバで実行された認証結果を受ける事で認証チケットが正当なものかの判断する判定ステップと、判定ステップで生成されたデータを認証端末へ返却するステップとからなる認証方法である。

【００１０】

この発明は、利用者が操作する認証を受ける複数の認証端末と、共通の認証サーバと、複数のサービス提供事業者とがネットワークを介して接続された認証システムにであって、
認証端末からユーザー認証の要求を受けた認証サーバが認証端末を操作する利用者の認証を行い、認証結果として生成されたデータを認証端末へ返却する第１認証手段と、
認証端末からの認証チケット要求のデータを受けた認証サーバが認証チケット発行のための認証を行い、認証結果として生成された認証チケットを含むデータを認証端末へ返却する第２認証手段と、
認証端末からの認証チケットを含むサービス提供要求のデータを認証端末から受けたサービス提供事業者サーバが認証チケットが正当なものかを判断するために行う第３認証手段とからなり、
第３認証手段は、サービス提供事業者自身が正当である事を証明するためのデータを含んだ認証チケット認証要求を認証サーバへ送信する送信手段と、認証サーバで実行された認証結果を受ける事で認証チケットが正当なものかの判断する判定手段と、判定手段で生成されたデータを認証端末へ返却する手段とからなる認証システムである。

【００１１】

この発明は、利用者が操作する認証を受ける複数の認証端末と、複数のサービス提供事業者とネットワークを介して接続され、認証端末およびサーバ提供事業者に対して共通の認証サーバであって、
認証端末からユーザー認証の要求を受け、認証端末を操作する利用者の認証を行い、認証結果として生成されたデータを認証端末へ返却する第１認証手段と、
認証端末からの認証チケット要求のデータを受け、認証チケット発行のための認証を行い、認証結果として生成された認証チケットを含むデータを認証端末へ返却する第２認証手段と、
認証端末からの認証チケットを含むサービス提供要求のデータを認証端末から受けたサービス提供事業者サーバが認証チケットが正当なものかを判断するために行う第３認証手段とからなり、
第３認証手段は、サービス提供事業者自身が正当である事を証明するためのデータを含んだ認証チケット認証要求をサービス提供事業者から受ける受信手段と、認証チケットが正当なものか否かを判断する判定手段と、判定手段で生成されたデータをサービス提供事業者に送信する手段とからなり、
サービス提供事業者が判定手段で生成されたデータを認証端末へ返却する認証サーバである。

【発明の効果】

【００１２】

第１の効果は、サービス提供事業者３００ のシステム構築，運用コストが大幅に軽減

される事である。

【００１３】

従来方式では、ネットワークサービス提供事業者が提供するディレクトリサービス等に則った方式に従う必要があったが、この発明による方式では、一般的によく知られているＨＴＴＰ(Hypertext Transfer Protocol)やＳＳＬ(Secure Socket Layer)でもシステム構築が可能である。また、サービス提供事業者側で構築が必要な部分は、本来以下の通りである。

【００１４】

１）サービスセッションＩＤの発行・送受信・管理

２）認証チケットの送受信とこの認証結果の送受信

３）サービス提供事業者ＩＤの認証サーバ６００ への送信

１）については、現在行っているネットワークを介したサービスが何かあれば、その仕組みを流用できるため、実質２）と３）の構築で済む事になる。このため、この発明によるシングルサインオン認証方式を用いる事で、サービス提供事業者は、従来方式と比較すると大幅なコスト軽減を実現できる。

【００１５】

また、サービス提供事業者が複数のネットワークサービス提供事業者と契約して、複数のネットワークサービス提供事業者の利用者へ向けてサービスの提供を行う場合も大幅なコスト削減が可能である。従来の方式では、それぞれのネットワークサービス提供事業者のシングルサインオン認証方式に沿ったシステム構築，運用が必要であったが、ネットワークサービス提供事業者のこの発明によるシングルサインオン方式は同じだが、ネットワークサービス提供事業者毎に認証チケットの形式を変える事が可能である。したがって、サービス提供事業者は認証チケットの形式を判別する事によって、どのネットワークサービス事業者の利用者からのアクセスであるかの判別ができるため、サービス提供事業者としては、一度のシステム構築で複数のネットワークサービス提供事業者の利用者へサービスを提供する事ができる。

【００１６】

第２の効果は、ネットワークサービス提供事業者がこの発明によるシングルサインオン認証方式でシステムを構築した場合、サービス提供事業者のサービスとしての参入障壁がかなり低くなる事である。第１の効果にも書いた通りであるが、システム構築が容易な事が理由である。

【００１７】

第３の効果は、セキュリティレベルの大幅な向上である。従来の方式では、認証サーバとの認証後に端末が認証サーバから取得するセッションＩＤを使って、端末が認証サーバや各サービス提供事業者サーバへアクセスしていたため、通信路上や端末、サービス提供事業者サーバからセッションＩＤを盗まれた場合、不正な利用者がこのＩＤを使って別端末から全てのサービス提供事業者サーバへアクセス可能であった。

【００１８】

しかしながら、この発明では、通信路上で送受信されるセッションＩＤが全て異なる種類であり、端末およびサービス提供事業者サーバ間のセッションを管理するために使用するサービスセッションＩＤは、サービス提供事業者サーバ毎に一意であり、セッション管理方式もサービス提供事業者毎に異なるため、仮に盗まれたとしても、不正な利用者が別端末からアクセスできる範囲を１つのサービス提供事業者サーバのみに抑える事ができる。

【００１９】

また、認証チケットが盗まれたとしても、認証チケットは、発行されてから数分間の有効期間しかないため、不正な利用者が認証チケットを盗んで不正利用する事は難しい。仮に、認証チケットを暗号化した場合、数分以内に復号して不正利用する事は、ほぼ不可能に近い。

【００２０】

第４の効果は、不正なサービス提供事業者をシステム的に排除できる事である。従来のシングルサインオン方式では、システム的にはサービス提供事業者サーバを基本的に信頼するしかなかったが、サービス提供事業者サーバが認証サーバへアクセスする際、上述のサービス提供事業者ＩＤを認証サーバへ送信する事を義務としているため、これで不正な事業者かどうかを判別する事ができる。

【００２１】

第５の効果は、認証チケットと様々なシステム・サービスとの連携の可能性がある事である。例えば、ネットワークサービス提供事業者毎に認証チケットの形式を変える事ができるので、サービス提供事業者は、認証チケットの形式を判別する事によって各ネットワークサービス提供事業者の利用者向けにサービスをカスタマイズする事もできる。

【００２２】

例えば、ネットワークサービス提供事業者を現在のインターネットプロバイダ，サービス提供事業者を各ＥＣ(Electronic Commerce:電子商取引)ショップと仮定すると、それぞれのプロバイダが発行する認証チケットの形式をプロバイダ毎に変える事で、ＥＣショップはどこのプロバイダからのアクセスかを知る事ができ、現ＥＣショップができないそれぞれのプロバイダのユーザー向けのサービスを展開する事が可能にもなる。

【００２３】

第６の効果は、利用者（端末)の認証だけでなく、サービス提供事業者の認証を認証チケットを発行しているネットワークサービス提供事業者が行っているため、不正なサービス提供事業者が利用者へ不正なサービスの提供を行った場合は即座にシステム的に情報通信ネットワークから切り離す事ができる事である。よって、利用者，ネットワークサービス提供事業者，サービス提供事業者の相互接続においては安全にネットワーク通信を行う事ができ、認証されていないサービス事業者のネットワーク通信を遮断する事ができ、本シングルサインオン認証方式を使用する事で、安全かつ柔軟性の高いネットワークサービス提供基盤の構築が可能となる。

【発明を実施するための最良の形態】

【００２４】

以下、この発明の実施形態について図面を参照して説明する。本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

【００２５】

第１認証ステップ：ユーザーＩＤ／パスワード等のユーザ認証情報を用いて認証サーバに対して利用者が行うユーザ認証の処理である。認証結果として生成されるデータは、認証許可情報（認証セッションＩＤ）または認証不許可情報である。

【００２６】

第２認証ステップ：認証端末からの認証チケット発行要求を受けた認証サーバが認証セッションＩＤによってその認証端末が正当な端末か否かを判定する処理である。正当と判定されると、認証チケットおよび認証セッションＩＤが端末へ返却される。

【００２７】

第３認証ステップ：サービス提供事業者サーバがサービス提供事業者自身が正当である事を証明するためのデータ（サービス提供事業者ＩＤ）を含んだ認証チケット認証要求を認証サーバへ送信し、認証サーバがサービス提供事業者および認証チケットを認証し、認証結果がサービス提供事業者に送信される。

【００２８】

図１は、この発明の一実施形態のシステム構成を示す。まず、システム構成として、利用者１００，ネットワークサービス提供事業者２００，サービス提供事業者３００の３つの要素からなる事を想定し、次の要素数，役割の関係からなるシステム構成を想定する。

【００２９】

１．要素数：

「利用者１００：ネットワークサービス提供事業者２００：サービス提供事業者３００

＝ｍ：１：ｎ」

【００３０】

２．役割：

１）利用者１００

ネットワークサービス提供事業者２００を通じて、サービスを受ける事ができる役割を持つ。尚、サービスを受ける場合は、如何なる場合においてもネットワークサービス提供事業者２００との契約を必要とする。逆に、各サービス提供事業者３００と直接契約を行わずとも、ネットワークサービス提供事業者２００と契約するだけでサービスを受ける事ができる。サービスの一例は、インターネットまたはイントラネットへの接続である。

【００３１】

２）ネットワークサービス提供事業者２００

利用者１００とサービス提供事業者２００を仲介する役割を持ち、利用者１００がサービスを受けるための一次窓口的な役割を担い、各サービス提供事業者３００と直接契約して利用者１００に対して各サービスへの入口と認証機能等の、利用者１００がサービスを受ける時に必要なセキュリティ機能やサービスを受ける利用者１００の利便性向上のための機能を提供する。また、サービス提供事業者３００と直接契約するか、ネットワークサービス提供事業者２００で直接サービスを構築し、利用者１００に対してサービスメニューの拡大をする事ができる。

【００３２】

３）サービス提供事業者３００

利用者１００へサービスそのものを提供する役割を持つ。利用者１００へサービスを提供する場合は、ネットワークサービス事業者２００と直接契約する必要がある。逆に、ネットワークサービス事業者２００と契約をしていれば、各利用者１００と直接契約をしなくとも、全ての利用者１００へサービスを提供する事ができる。

【００３３】

次に、このビジネスモデルを実現するためのシステム構成を想定する。個別要素，要素数，役割は次の通りである。

【００３４】

１．要素数：

「端末５００：認証サーバ６００：サービス提供事業者サーバ７００＝ｍ：１：ｎ」。

【００３５】

２．役割：

１）端末５００

利用者１００がサービスを受けるために必要な機能を持ち、情報通信ネットワーク５０に接続されたシステム，プログラム，装置である。構成例において、一実施形態のシングルサインオン認証方式の端末機能（下記に示す）を持つものは全て対象となる。

【００３６】

(a)認証サーバ６００へのユーザー認証の要求（ユーザー認証情報の送信を含む）機能

(b)認証サーバ６００との認証セッション持続機能

(c)認証サーバ６００への認証チケットの要求機能

(d)サービス提供事業者サーバ７００への認証チケットによる認証の要求（認証チケットの送信）機能

(e)(a)～(d)の応答結果に関する処理機能。

【００３７】

２）認証サーバ６００

サービス提供事業者サーバ７００が端末５００へサービスを行う時に必要なセキュリティ機能やサービスを受ける利用者１００の利便性向上のための機能（下記に示す）を持ち、情報通信ネットワーク５０に接続されたネットワークサービス事業者２００が持つシステム，ソフトウェア，装置である。

【００３８】

(a)端末５００からのユーザー認証の要求に基づき、ユーザー認証処理を行い、認証結果を返却する機能
(b)端末５００との認証セッション持続・管理機能
(c)サービス提供事業者サーバ７００の認証・管理機能
(d)端末５００から認証チケット要求を受け、認証チケットを発行し、端末５００へ返却する機能
(e)サービス提供事業者サーバ７００からの認証チケット確認要求を受け、認証チケットが正当なものであるかどうかの確認・認証を行い、認証結果をサービス事業者サーバ７００へ返却する機能
(f)利用者１００へサービスを提供する前に行われるサービス提供事業者サーバ７００からの正規登録要求を受け、正規のサービス提供事業者３００として登録を行い、サービス提供事業者サーバ７００へサービス提供事業者ＩＤを発行する機能。

【００３９】

３）サービス提供事業者サーバ７００

端末５００と接続して利用者１００へサービスを提供し、利用者１００・端末５００の認証のために認証サーバ６００と接続をするための機能（下記に示す）を持ち、情報通信ネットワーク５０に接続されたシステム，プログラム，装置である。

【００４０】

(a)端末５００からの認証チケットによる認証要求を受け、認証サーバ６００に正当性の確認・認証のための要求を送信し、その返却結果を受ける機能
(b)(a)で受けた返却結果を判断し、端末５００に認証結果を返却する機能。

【００４１】

４）情報通信ネットワーク５０

端末５００，認証サーバ６００，サービス提供事業者サーバ７００を相互に接続するために必要である。一実施形態のシングルサインオン認証方式が実現可能なデジタルデータの送受信が可能な情報通信ネットワークであり、インターネットまたはイントラネットである。

【００４２】

上述したこの発明の一実施形態の動作について、図１を参照して説明する。その後、図２を用いて動作の詳細について説明する。また、ここで説明している通信路はセキュリティの観点から全て暗号化されているものとする。尚、ここで使用している用語の意味は、次の通りである。

【００４３】

１．ログイン操作

利用者１００がユーザーＩＤ／パスワードを用いて、認証サーバに対して認証要求を行う事がログイン操作である。この認証結果次第で利用者１００がネットワークサービスへアクセス可能かどうかが判別される。例えばユーザーＩＤ／パスワードは、複数のサービス提供事業者に対して共通のものとされている。

【００４４】

２．認証チケット

端末５００－認証サーバ６００－サービス提供事業者サーバ７００間の一実施形態によるシングルサインオン認証方式で使用される中核的な役割を果たすものであり、認証チケットの機能・要件は次の通りである。尚、各接続セッションと認証の相関関係については、図３に示し、後述する。

【００４５】

１）認証サーバ６００によって認証許可された端末５００へのみに発行されるユーザー認証情報を含まない一意に異なるＩＤ（データ）であり、その形態は様々である。

【００４６】

２）認証チケットは、一度しか使用する事（認証サーバ６００による認証）ができないワンタイムなものである。

【００４７】
３）認証チケットが発行されてから認証を行うまでの間に有効期間が設けられており、発行されてから有効期間（図２中の(Ａ１７)で発行されて(Ａ２１)で確認されるまでの時間に有効期間例えば数分間が設定されている。）内に認証サーバ６００へ認証チケットの確認要求が来ない場合は自動的に無効となる。また、有効期間内に確認された場合でも、それ以降この認証チケットが使用される事はないため、認証サーバ６００内で破棄する。これは、２）の理由もあるが、認証チケットの不正利用を防止するための対策でもある。
【００４８】
４）認証チケットが一意に異なるＩＤであるため、端末５００，サービス提供事業者サーバ７００が別の仕様用途で利用する事についても問題ないものとなっている。有効期間が設定されており、ワンタイムなものであるため、認証チケットを保存して、後で不正な認証のために使用する事ができない仕組みとなっているため、問題ない。
【００４９】
５）必要に応じて署名を付加したり、暗号化を行う場合もある。
【００５０】
３．認証セッションＩＤ
端末５００と認証サーバ６００の間で利用者１００の認証が正常完了した場合に認証サーバ６００から端末５００へ発行される一意なＩＤが認証セッションＩＤである。認証セッションＩＤを保持している端末は、利用者１００による認証が正常に完了したとみなされる。
【００５１】
認証セッションＩＤは、ユーザーＩＤ，パスワード，機器種別情報，機器固有情報，チャレンジフレーズ等をいくつか組合せて使った利用者１００に認証情報を手入力させて行う認証である。尚、認証セッションＩＤに、機器毎に一意なＩＤ情報を入れたり、認証チケット自体を入れる事も考慮され、認証セッションＩＤ自体も有効期間を持ち、必要に応じて署名を付けたり、暗号化を行う場合もある。
【００５２】
４．サービスセッションＩＤ
端末５００から送られてきた認証チケットを受け取ったサービス提供事業者サーバ７００が、端末５００から送られてきた認証チケットの確認・認証の要求を認証サーバ６００に対して行い、認証サーバ６００による認証が成功した時にサービス提供事業者サーバ７００が端末５００に対して発行する一意なＩＤがサービスセッションＩＤである。
【００５３】
サービスセッションＩＤを保持している端末は、サービス提供事業者サーバ７００が認証サーバ６００へ正当であるかどうかの認証を行った端末とみなせる。尚、サービスセッションＩＤに、機器毎に一意なＩＤ情報を入れたり、認証チケット自体を入れる事も考慮され、サービスセッションＩＤ自体も有効期間を持ち、必要に応じて署名を付けたり、暗号化を行う場合もある。
【００５４】
５．サービス提供事業者ＩＤ
サービス提供事業者が利用者１００へサービスを提供する前に、事前に認証サーバ６００へサービス提供時に使用するサービス提供事業者サーバ７００を正規登録し、正規登録が完了した時に認証サーバ６００から発行される正当なサービス提供事業者である事を示す一意なＩＤがサービス提供事業者ＩＤである。
【００５５】
利用者１００へサービスを提供する前に発行を受ける必要のあるＩＤである。認証サーバ６００から発行を受けていない場合は、正規のサービス提供事業者とみなされないため、利用者１００へサービスを提供する事ができない。尚、サービス提供事業者ＩＤには有効期間を設定する事が可能であり、有効期間が設定されている場合は、有効期間が切れた後、再度正規登録が必要である。また、必要に応じて署名を付けたり、暗号化を行う場合

もある。

【００５６】

また、サービス提供事業者ＩＤの取得方法として、システム的に認証サーバ６００と接続してネットワークサービス提供事業者２００から受け取るという事に限らず、サービス提供事業者ＩＤを取得するためのシステム的な手段をサービス提供事業者３００が持たなくても、ネットワークサービス提供事業者２００との契約時に何かしらの代替手段によりサービス提供事業者ＩＤを取得することが可能である。

【００５７】

図３は、各認証とセッションの相関関係を示す。利用者１００からのログイン操作、すなわち、端末５００からのユーザＩＤ／パスワードの送信により、認証が許可され、認証サーバ６００から発行される認証セッションＩＤによって、端末５００および認証サーバ６００間のセッションＳ１０が維持される。利用者１００の明示的なログアウト、認証セッションのタイムアウト、異常発生によるネットワーク切断等によって認証セッションＳ１０が切断される。

【００５８】

サービス提供事業者３００が利用者１００からのアクセス要求（端末５００が認証チケットを送信）を受け、サービス提供事業者３００がアクセス要求を判断する。すなわち、サービス提供事業者サーバ７００が端末５００から受信した認証チケットを認証サーバ６００へ送信・確認する。その結果、アクセスが許可されると、サービス提供事業者サーバ７００から発行されるサービスセッションＩＤによって、端末５００およびサービス提供事業者サーバ７００間のセッションＳ１１が維持される。利用者１００の明示的なログアウト、認証セッションのタイムアウト、異常発生によるネットワーク切断等によってサービスセッションＳ１１が切断される。

【００５９】

ネットワークサービス提供事業者２００とサービス提供事業者３００との間のセッションＳ１２は、特に維持される事がないが、ネットワークサービス提供事業者２００がサービス提供事業者３００と契約する時に採番したサービス提供事業者ＩＤを、サービス提供事業者サーバ７００が認証サーバ６００へアクセスする時に送信する事により、認証サーバ６００は、アクセス可否を判断する。

【００６０】

この発明の一実施形態の動作を説明する。

【００６１】

１．利用者１００がネットワークサービスへアクセスする時、認証サーバ６００に対してログイン操作を行う。ログインの際、利用者１００はユーザーＩＤ／パスワードによるユーザー認証を行う。認証が正常に完了したら、端末５００は認証サーバ６００から認証許可情報（以下、認証セッションＩＤ）を受信する。以後、端末５００－認証サーバ６００の通信時は必ず認証セッションＩＤを用いて行われ、この両者間のみに有効なものである。また、認証セッションＩＤは端末５００毎に一意に異なる。認証セッションＩＤが無効となった場合（利用者１００の明示的なログアウト，認証セッション保持期間切れによるセッション自動切断等が起きた場合）、利用者１００は再度ログイン操作を行う。

【００６２】

２．ログインを行った後、利用者１００は提供を受けたいサービスを選択する。尚、サービスを選択してサービス提供事業者サーバ７００へアクセスしに行く場合、サービス提供事業者サーバ７００に対して認証チケットを送信する必要があるため、事前に認証サーバ６００から認証チケットを取得しておく。ここで、認証サーバ６００から認証チケットを受け取る事ができない場合は、上記１の認証セッションＩＤが無効となっているため、利用者１００は再度ログイン操作を行う必要がある。

【００６３】

３．利用者１００は、サービス選択後、認証サーバ６００から受け取った認証チケットをサービス提供事業者サーバ７００へ送信する。

【００６４】
４．サービス提供事業者サーバ７００は認証チケットを受け取ったら、認証サーバ６００に確認の要求を出して結果を受け取る。認証サーバ６００による確認の結果、認証チケットが正しいものであると判別されたら、端末５００へサービス提供許可情報（以下、サービスセッションＩＤ）を送信する。認証チケットに問題ありと判別されたら、端末５００へ問題の内容（エラー情報）を送信する。
【００６５】
５．端末５００はサービスセッションＩＤを受け取ったら、サービス提供事業者サーバ７００からサービスを受ける事ができる。エラー情報を受け取ったら、利用者１００によるログイン操作の実施や認証チケット再取得を行う。尚、サービスセッションＩＤは端末５００－サービス事業者サーバ７００間毎に一意であり、サービスセッションＩＤが無効となった場合（認証セッションＩＤと同様の場合）も、利用者１００はログイン操作の実施や、認証チケット再取得を行う。ここではサービスセッションＩＤの形式は問わないが、認証チケットを含む場合も考慮される。
【００６６】
次に、この発明の一実施形態のより詳細な動作について図２を参照して説明する。尚、図２中に書かれている(Ａ１０)のような参照符号は、それぞれの動作に対応して振られており、(Ａ１０)～(Ａ２７)までである。この１つずつの動作が全て組み合わされる事により、一実施形態によるシングルサインオン認証方式が実現される事になる。
【００６７】
１．ステップＡ１０において、利用者１００がログイン操作時に入力したユーザーＩＤ／パスワード（ユーザー認証情報）を端末５００が認証サーバ６００へ送信する。送信後、端末５００は、認証サーバ６００から認証結果が返却されるまで待機状態へと遷移する。
【００６８】
２．ステップＡ１１において、ユーザー認証情報を受け取った認証サーバ６００は、この情報を基にユーザー認証処理を実行し、認証処理結果を得る。この結果、認証不許可であれば、認証が不許可となった旨を端末５００へ通知する（ステップＡ１２）。認証許可の場合であれば、端末５００へ許可の通知と共に認証セッションＩＤを返却する（ステップＡ１４）。
【００６９】
３．待機状態となっていた端末５００は、認証不許可の通知を受信した場合は、利用者１００へ画面を通してその旨を通知する（ステップＡ１３）。認証許可の通知を受信した場合は、共に受信した認証セッションＩＤを使ってセッションの確立処理を行い、認証セッションＩＤを端末５００に保存する（ステップＡ１５）。このステップＡ１５までの処理が利用者認証であり、以下が認証チケットによる認証である。
【００７０】
４．ユーザー認証が終わった後、利用者１００は受けるサービスを選択するが、サービスを受けるためには認証チケットを取得しなければならない。そこで、ステップＡ１６において、端末５００が認証サーバ６００へ認証チケットの要求を送信する。同時に、認証サーバ６００へアクセスするために必要な認証セッションＩＤも送信する。送信後、要求結果が返却されるまで待機状態へと遷移する。
【００７１】
５．端末５００から認証チケットの要求を受け取った認証サーバ６００は、同時に受信した認証セッションＩＤにより、正当な端末５００からのアクセスであるかどうかを判定し、正当な端末であると判断した後、ステップＡ１７において、端末５００へ返却するための認証チケットを発行し、発行した認証チケットを認証サーバ６００自身でも保持する。
【００７２】
６．ステップＡ１８において、認証サーバ６００は、発行した認証チケットを端末５０

０へ返却する。同時に認証セッションＩＤも返却する。

【００７３】

７．待機状態となっていた端末５００は、認証チケットと認証セッションＩＤを受信する。ここで、認証セッションＩＤが端末内に保存しておいたものと同一かを確認し、同一であれば、ステップＡ１９において、利用者１００が上述した４の段階で選択したサービス提供事業者サーバ７００へ、サービス提供例えばネットワークへの接続の要求と認証チケットを送信する。送信後、端末５００は認証チケットを削除し、待機状態へと遷移する。

【００７４】

８．端末５００から認証チケットを受け取ったサービス提供事業者サーバ７００は、ステップＡ２０において、送信されてきた認証チケットが正当なものであるかを判断するため、認証サーバ６００へ認証チケットを送信し、返却結果を待つ。同時に、サービス提供事業者３００が正当である事を表すサービス提供事業者ＩＤも送信する。尚、認証サーバ６００に認証チケットを送信後、受信した認証チケットを削除し、待機状態へと遷移する。

【００７５】

９．サービス提供事業者サーバ７００から認証チケットとサービス提供事業者ＩＤを受信した認証サーバ６００は、ステップＡ２１において、まずサービス提供事業者ＩＤが正当なものであるかを判断する。サービス提供事業者ＩＤが正当なものであれば、次に認証チケットの認証を行う。認証の結果、認証サーバ６００自身で発行した事，有効期間内に認証が完了した事が確認する事ができれば認証正常終了とする。

【００７６】

１０．認証処理が完了した場合、どのような結果の場合であっても、認証結果をサービス提供事業者サーバ７００へ通知する（ステップＡ２２）。

【００７７】

１１．待機状態となっていたサービス提供事業者サーバ７００は、ステップＡ２３において、受信した認証チケットの認証結果を判断し、この判断結果を得る。判断結果が認証許可であった場合は、ステップＡ２６において、端末５００へ許可の通知と共にサービス提供事業者サーバ７００がサービスセッションＩＤを発行し、端末５００を返却する。認証不許可であった場合は、ステップＡ２４において、端末５００に対して不許可の通知を行う。

【００７８】

１２．待機状態であった端末５００は、認証許可の通知を受信した場合は、共に受信したサービスセッションＩＤを使ってセッションの確立処理を行い、サービスセッションＩＤを端末５００内に保存する（ステップＡ２７）。認証不許可の通知を受信した場合は、利用者１００へ画面を通してその旨を通知する（ステップＡ２５）。

【００７９】

次に、この発明の他の実施形態について説明する。他の実施形態では、以下に述べるような各ユーザーの嗜好に応じた広告情報を送信するようにしたものである。尚、上述した一実施形態のシステム構成およびシングルサインオン認証方法は、他の実施形態においても同様に適用されている。

【００８０】

まず、認証サーバは、例えば図４に示すようなユーザー情報に関するデータベースを保持するものとする。図４に示されるデータベースについてユーザー名、ユーザーＩＤ、パスワードは各ユーザーの登録時に記録されることになる。

【００８１】

サービス利用履歴情報は、各ユーザーが種々のサービス提供事業者サーバにアクセスすることにより、どの様なサービスを利用したかを記録するためのものである。サービス利用履歴情報を記録する方法としては、サービス提供事業者サーバによるサービス提供が完了したときに、ユーザーまたはサービス提供事業者サーバから認証サーバへサービス利用

履歴情報および記録要求を送信することにより記録する方法等が考えられる。

【００８２】

ユーザー嗜好情報は、各ユーザーの嗜好情報をキーワードとして記録するためのものである。ユーザー嗜好情報を記録する方法としては、認証サーバが前述のサービス利用履歴情報からキーワードを抽出する方法、またはユーザーまたはサービス提供事業者サーバから認証サーバへユーザー嗜好情報および記録要求を送信することにより記録する方法等が考えられる。

【００８３】

そして、任意のサービス提供事業者サーバは、広告情報を送信する。具体的には広告したい商品やサービスの商品情報・サービス情報および広告要求を認証サーバに送信する。その際には、その商品・サービスに関連するキーワードが含まれていてもよい。商品情報・サービス情報またはキーワードを受信した認証サーバは、それらの情報と前述し、図４に示す自身が保持するデータベースに含まれるユーザー嗜好情報とを比較する。この時、データベース内の全てのユーザーのユーザー嗜好情報を比較対象とする。すなわち、広告要求を送信したサービス提供事業者サーバを過去に利用したことのないユーザーも比較対象となる。

【００８４】

次に、商品情報・サービス情報またはキーワードとユーザー嗜好情報とが一致したユーザーに対してのみ広告情報を送信する。

【００８５】

このようにすることで不特定多数のユーザーおよびサービス提供事業者サーバ間で商品やサービスの利用機会を広げることができる。

【００８６】

さらに、以下に述べるような実施形態も可能である。

【００８７】

認証サーバがユーザーに対して認証チケットを発行するときに、認証チケットとともにデータベース内のユーザー嗜好情報を送信する。このユーザー嗜好情報は暗号化されていることが望ましい。

【００８８】

そして、ユーザーがサービス事業者へアクセスするときに、そのユーザー嗜好情報を送信する。それにより、そのサービス事業者へ初めてアクセスする場合であっても、そのサービス事業者はユーザー嗜好情報を瞬時に把握・保持することができる。そして、そのユーザー嗜好情報に基づいてサービス事業者から直接に提供する商品やサービスを利用する可能性が高いユーザーへ広告情報を送信することができる。

【００８９】

また、サービス事業者が認証サーバに対して認証チケットの認証要求を行い、認証結果を受信するときに認証サーバが保持するデータベース内のユーザー嗜好情報も受信するようにしても良い。

【００９０】

この発明は、上述したこの発明の一実施形態等に限定されるものでは無く、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばサービス提供事業者は、接続サービス以外のサービスを提供するＷＷＷサーバであっても良い。

【図面の簡単な説明】

【００９１】

【図１】この発明による認証システムの一実施形態の構成を示すブロック図である。

【図２】この発明の一実施形態の処理の流れを説明するフローチャートである。

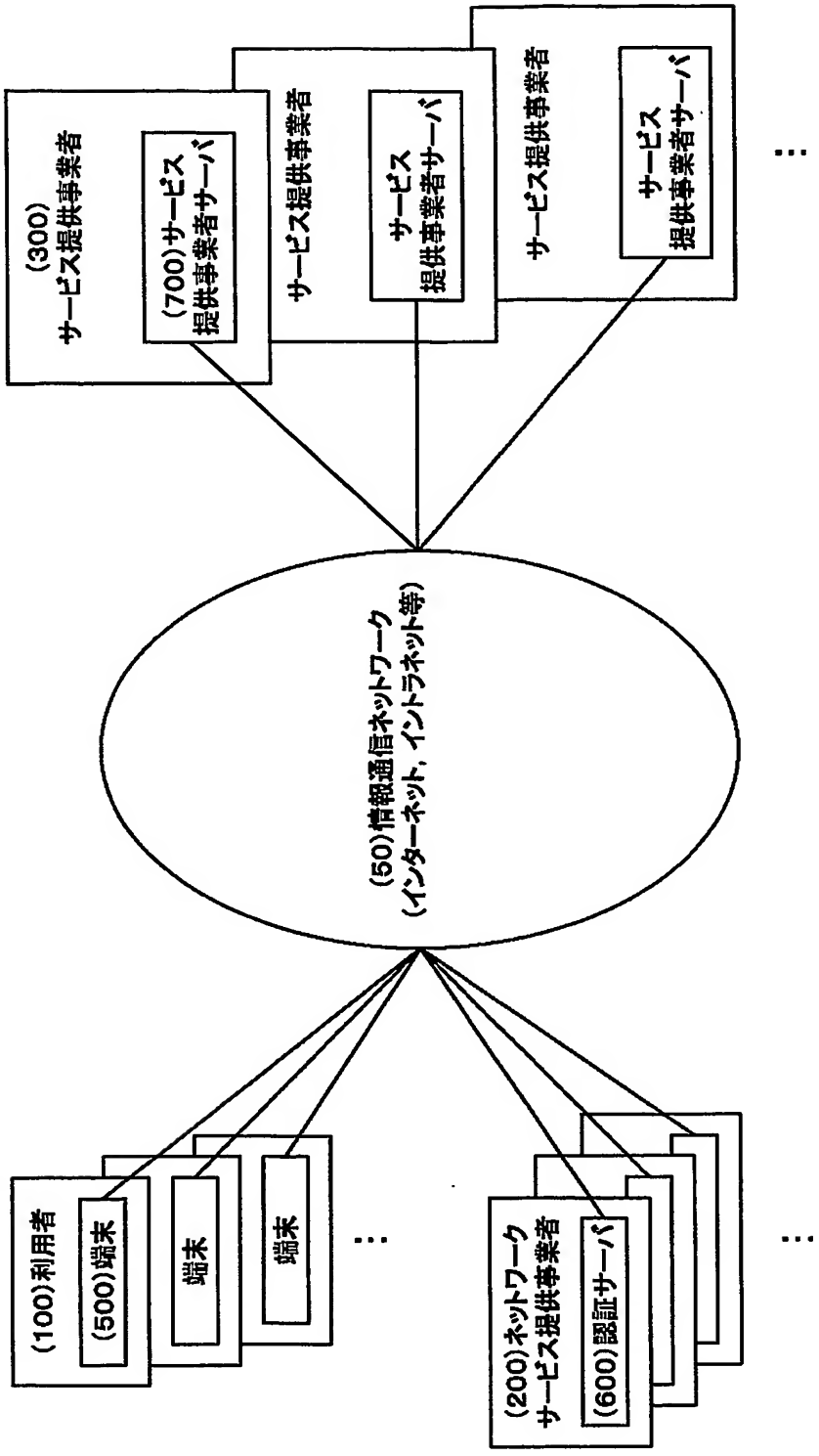
【図３】この発明の一実施形態における認証と請求項の相関関係を示す略線図である。

【図４】認証サーバが備えるデータベースの説明に用いる略線図である。

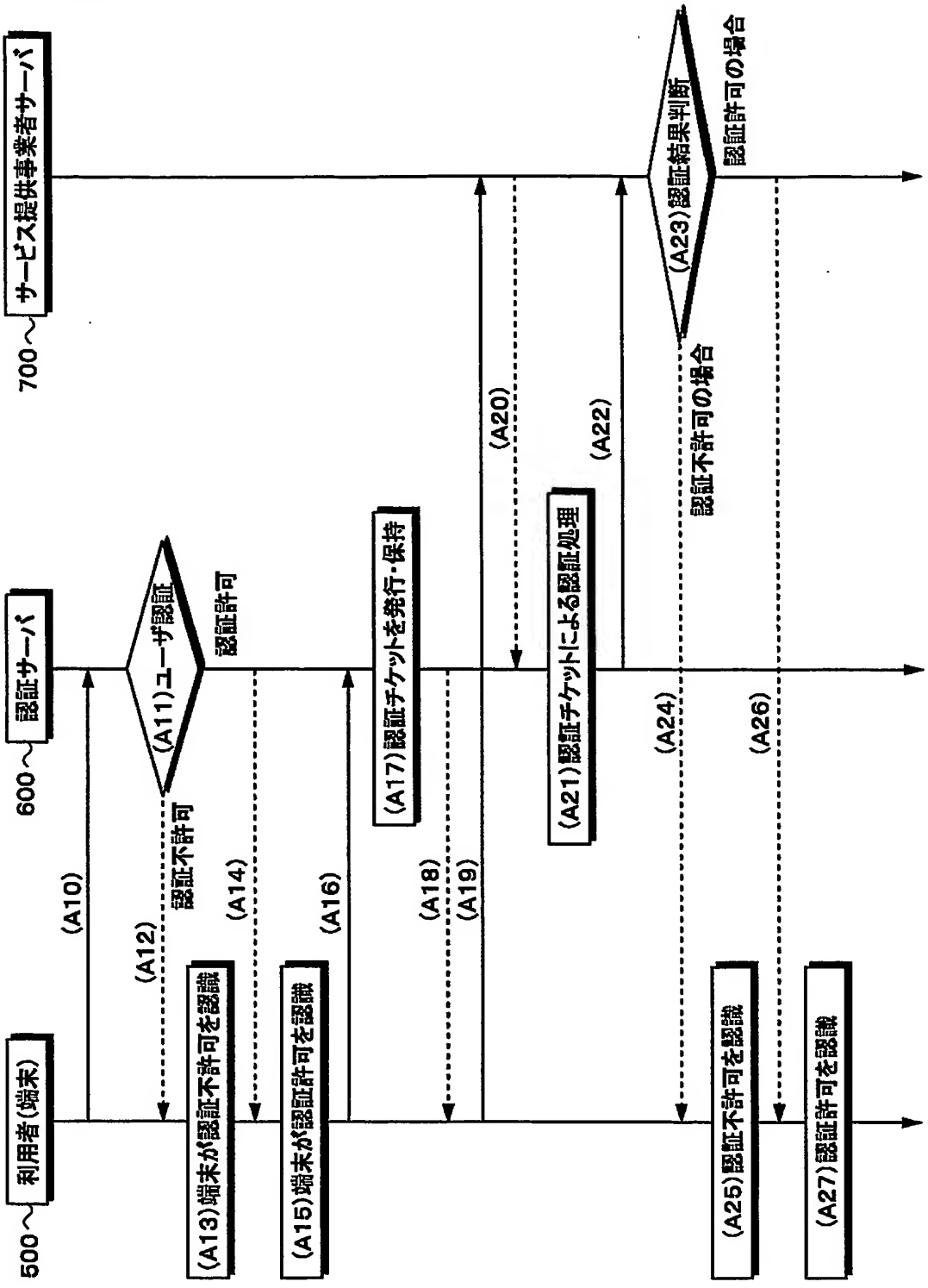
【符号の説明】

【００９２】
５０　　情報通信ネットワーク
１００　利用者
２００　ネットワークサービス提供事業者
３００　サービス提供事業者
５００　端末
６００　認証サーバ
７００　サービス提供事業者サーバ

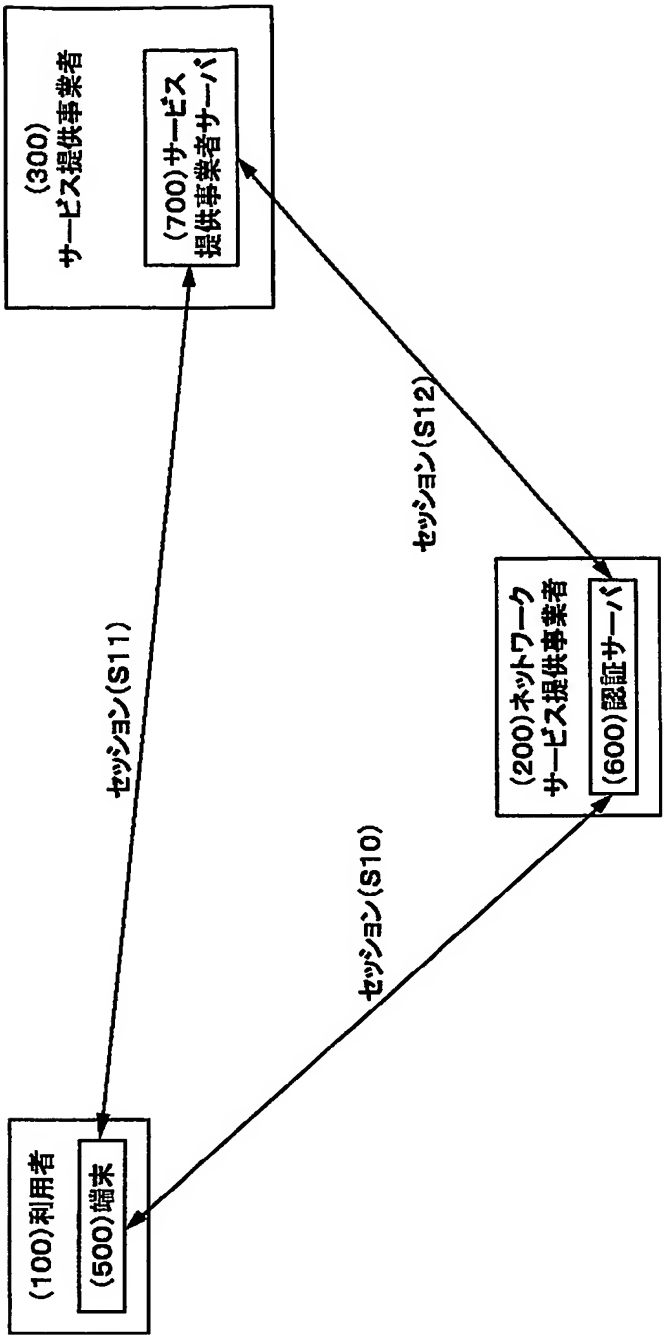
【書類名】図面
【図１】


(300)
サービス提供事業者
(700)サービス
提供事業者サーバ
サービス提供事業者
サービス
提供事業者サーバ
サービス提供事業者
サービス
提供事業者サーバ
(50)情報通信ネットワーク
(インターネット、イントラネット等)
(100)利用者
(500)端末
端末
端末
(200)ネットワーク
サービス提供事業者
(600)認証サーバ

【図２】


700
サービス提供事業者サーバ
600
認証サーバ
500
利用者(端末)
(A10)
(A11)ユーザ認証
認証許可
認証不許可
(A12)
(A13)端末が認証不許可を認識
(A14)
(A15)端末が認証許可を認識
(A16)
(A17)認証チケットを発行・保持
(A18)
(A19)
(A20)
(A21)認証チケットによる認証処理
(A22)
(A23)認証結果判断
認証許可の場合
認証不許可の場合
(A24)
(A25)認証不許可を認識
(A26)
(A27)認証許可を認識

【図３】


(300)
サービス提供事業者
(700)サービス
提供事業者サーバ
セッション(S12)
セッション(S11)
(200)ネットワーク
サービス提供事業者
(600)認証サーバ
セッション(S10)
(100)利用者
(500)端末

【図４】

ユーザ名	ユーザID	パスワード	サービス利用履歴情報		ユーザ嗜好情報
山田幸弘	01587638	atlantic	02’／08／30 浜崎あゆみ HANABI オンライン音楽購入 サービス提供事業者ID4利用	02’／11／08 宇多田ヒカル FINAL DISTANCE CD購入 サービス提供事業者ID1利用	浜崎あゆみ、 宇多田ヒカル、 ポップス、 ヒットチャート
平川悦子	01497635	pacifio	03’／06／07 JAL JAL497便 エアチケット購入 サービス提供事業者ID3利用	03’／04／25 メリディアン バンコク ホテル予約 サービス提供事業者ID2利用	旅行、 ホテル、 エスニック、 バカンス

【書類名】要約書
【要約】
【課題】　利用者の利便性を向上し、サービス提供事業者のシステム構築のコストおよび運用管理コストの低減を可能とする。
【解決手段】　ユーザー認証処理が実行され、端末500へ認証セッションＩＤが返却される(A14)。認証サーバ600が認証チケットを発行・保持する(A17)。認証チケットおよび認証セッションを端末500へ返却する(A18)。利用者100がサービス提供事業者サーバ700へサービス提供の要求と認証チケットを送信し、サービス提供事業者サーバ700が認証サーバ600へ認証チケットを送信する(A200)。認証サーバ600が認証チケットの認証処理を行い(A21)、認証結果が通知される(A22)。認証許可の場合は、許可の通知と共にサービスセッションＩＤが発行される(A23)。認証許可の通知が受信されると、端末500が受信したサービスセッションＩＤを使ってセッションの確立処理を行い、サービスセッションＩＤを保存する(A27)。
【選択図】　図２

特願２００３－２９１７４１

出　願　人　履　歴　情　報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社